NDIA

CMMC
Implementation Update
&
Ask the Experts

Current As Of: 16 February 2023

Sponsored by: abacode
Cybersecurity & Compliance

NDIA

If you care about CMMC…

NDIA New England Chapter 7th Annual Cyber Event

Protecting our Advantage:

CMMC, Cybersecurity Compliance, and Resilience

10 May 2023

Gillette Stadium, Foxborough, MA

For more information visit: ndianewengland.org

Sponsored by: abacode
Cybersecurity & Compliance

TODAY'S SPEAKERS

Amira Armond

President

Kieri Solutions
Vice Chair, C3PAO Stakeholder Forum

Vince Scott

CEO

Defense Cybersecurity Group
INFRAGARD National SME Cyberwarfare

Ryan Heidorn

Chief Technology Officer

C3 Integrated Solutions
Board Director, NDIA New England

Alex Major

Attorney

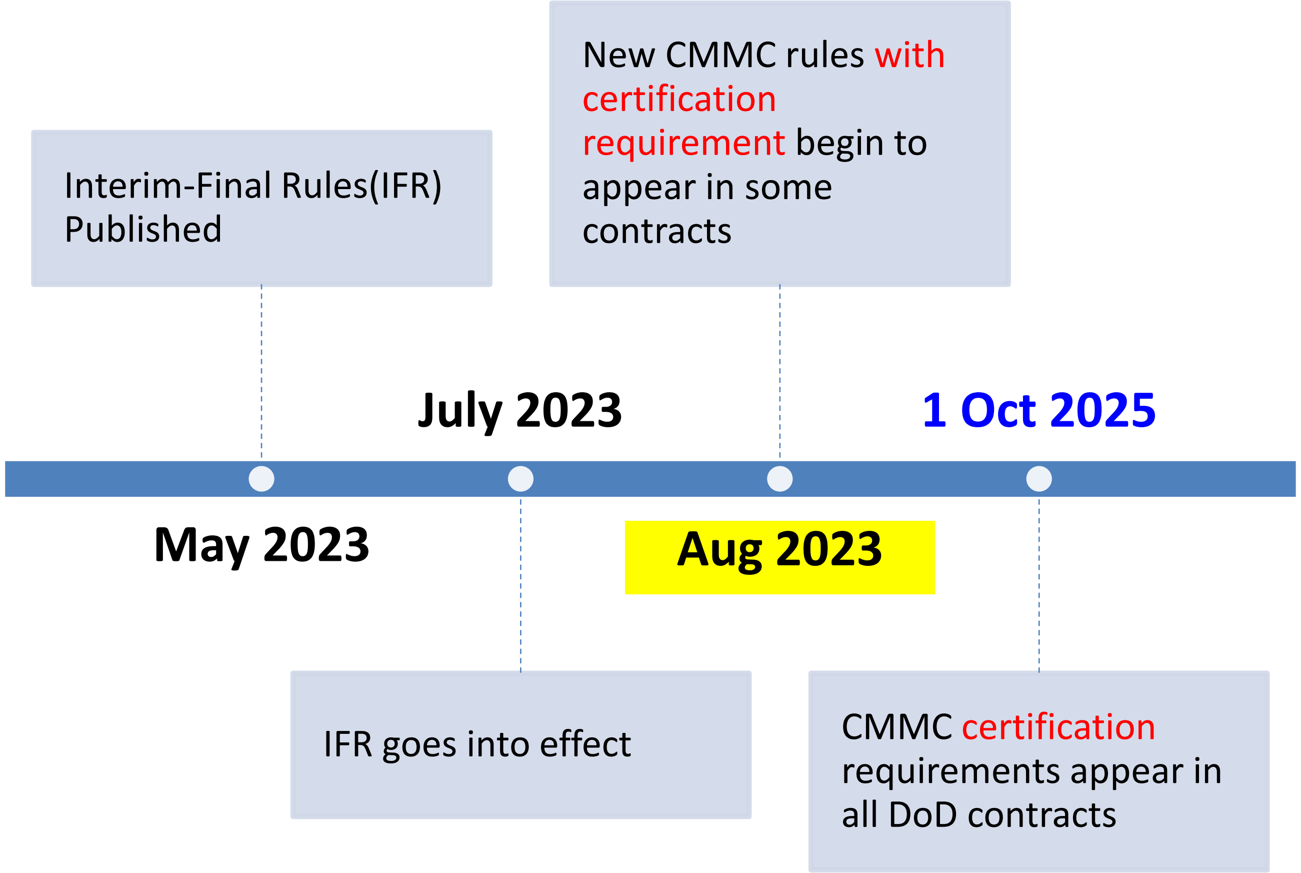
McCarter and English

Sponsored by: abacode
Cybersecurity & Compliance

Interim Final Rule

CMMC Rulemaking

- **What we expected prior to Feb 23**
- Executive Order 12866 (1993) requires annual production of a Unified Regulatory Agenda and Regulatory Plan
  - Office of Information and Regulatory Affairs (OIRA) published fall Unified Agenda late Dec 22
- In Dec 22 Agenda OIRA listed modification to DFARS (48CFR) as a change to CMMC requirements previously issued as an Interim Final Rule (IFR) in Sep 20
- OIRA also listed new proposed rule to create CMMC Program in Title 32



May 2023: Interim-Final Rules(IFR) Published

July 2023: IFR goes into effect

Aug 2023: New CMMC rules with certification requirement begin to appear in some contracts

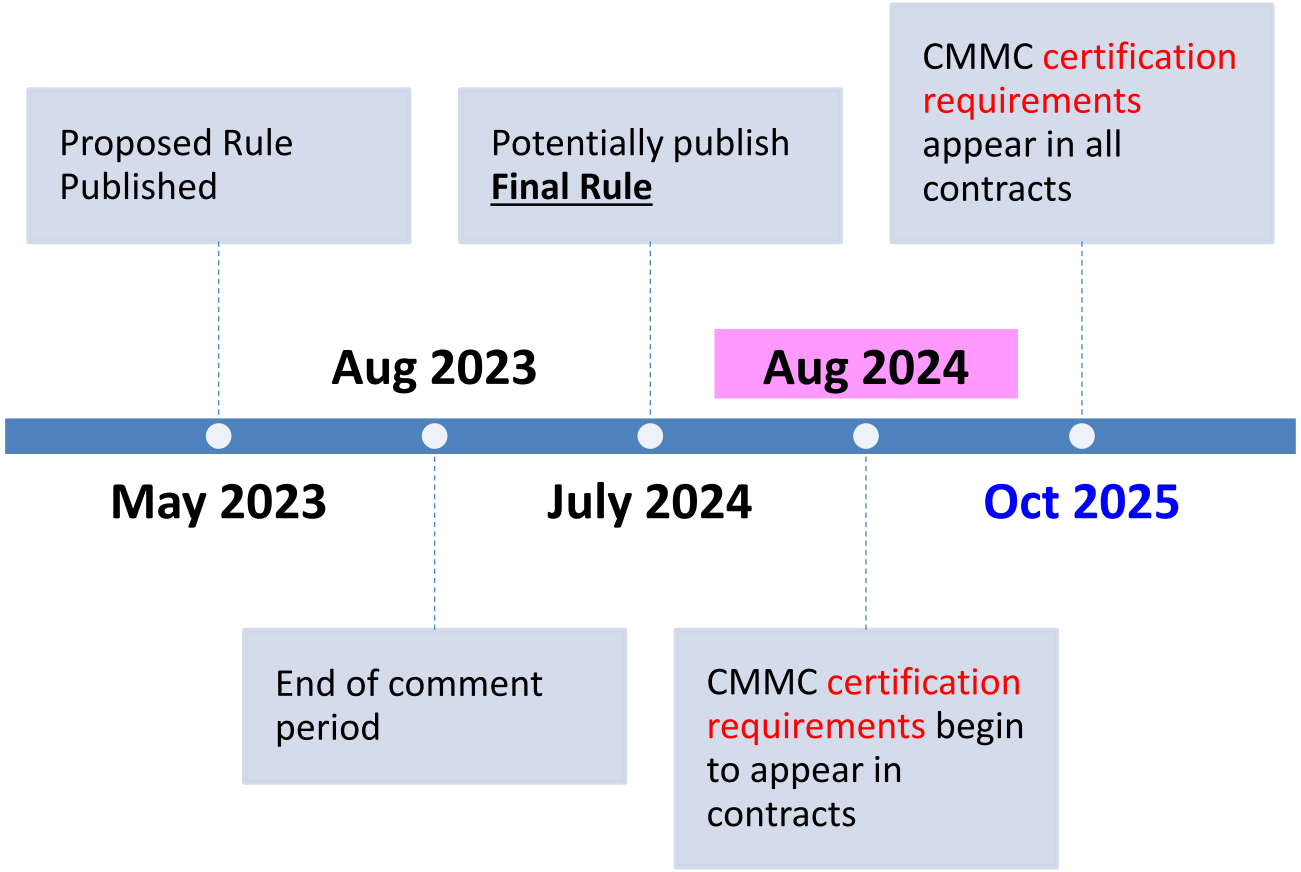
1 Oct 2025: CMMC certification requirements appear in all DoD contracts

Sponsored by: abacode Cybersecurity & Compliance

Proposed Rule

CMMC Rulemaking

- **What we now think is possible**
- IFR: rule goes into effect 60 days after publication & can begin to appear in contracts
- Proposed Rule
  - Usual /normal way rule changes are enacted
  - Requires comment period
- After comment period DoD must:
  - Adjudicate comments
  - Adjust rule if they deem appropriate
  - Publish final rule & include reasoning and approach to comments
- **What is the difference?**
  - Aug 23 vs Aug 24 for required 3rd party assessments to appear in contracts
- Overall end date for full implementation, 1 Oct 25 (beginning of FY26) remains unchanged from outline in DFARS 204.7503



May 2023: Proposed Rule Published

Aug 2023: End of comment period

July 2024: Potentially publish **Final Rule**

Aug 2024: CMMC certification requirements begin to appear in contracts

Oct 2025: CMMC certification requirements appear in all contracts

Sponsored by:

abacode
Cybersecurity & Compliance

Secure Your Networks and Systems In Physical Space and Cyberspace

NDIA

- **Secure your Networks. Now**
- DFARS 7012 / NIST 800-171 impose current Contractual Obligations
- Self-Assessment did not incentivize companies to comply
  - Does not negate obligation to meet the Standards in the Cybersecurity Framework

Sponsored by: abacode Cybersecurity & Compliance

Secure Your Networks and Systems In Physical Space and Cyberspace

- **Be prepared for uncertainty**
  - Follow your contractual requirements
  - Meet all existing cybersecurity obligations
    - FCI vs. CUI vs. CDI
  - Remain “current, accurate, and complete”
  - Government’s lack of clarity is dangerous
    - Communicate effectively – to all
- **Enforcement and Oversight**
  - What mechanisms/tools outside of NIST/CMMC can/will the government use to ensure compliance?
    - Prime contractor arm-pulling?
    - Hold back?
    - False Claims Act?
    - Specialized clauses - NMCARS 5204.73
      - “material requirement.”

Sponsored by: abacode

Cybersecurity & Compliance

NDIA Recommendations

NDIA

- Current plan as NDIA understands it will result in significant failure rates across the DIB (and government)
- 3 Recommendations

1. DoD CIO include industry in their assessment plan
   - Without correction, 1st year assessments could carry 75%+ failure rate
   - Likely to drive industry opt outs, anger & additional congressional oversight
2. Assess MSPs as part of a cohesive strategy
   - Verify providers meet standards on behalf of their clients
3. Adjust implementation plan – Move away from cliff implementation
   - Max 10% / 11 controls auto-fails
   - 80% of 110 controls = PASS
   - Consider further adjustments for small business

Sponsored by:

abacode
Cybersecurity & Compliance

Secure Your Networks and Systems In Physical Space and Cyberspace

- **Be working on these controls now!**
  - 18-24 months a reasonable, serious timeline; lower costs
  - 7 months a crash program with heavy investment
  - 7 days / 7 weeks un-executable at any cost
- Prioritize!
  - Some controls provide larger impact
  - 100% implementation extremely difficult

NDIA

Questions?

Sponsored by: abacode

Cybersecurity & Compliance